Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 3

Carlos Gustavo Moreira

Aula 12

Descenso infinito de Fermat

1 Descenso Infinito de Fermat

Dada uma equação

$$f(x_1, \ldots, x_n) = 0,$$

o método do descenso infinito (quando aplicável) permite mostrar que esta equação não possui soluções inteiras positivas ou, sob certas condições, até mesmo encontrar todas as suas soluções inteiras. Se o conjunto de soluções de f

$$A = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid f(x_1, \ldots, x_n) = 0\}$$

é diferente de vazio, então gostaríamos de considerar a solução "mínima" em certo sentido. Em outras palavras, queremos construir uma função $\phi\colon A \to \mathbb{N}$ e considerar a solução $(x_1, \ldots, x_n) \in A$ com $\phi(x_1, \ldots, x_n)$ mínimo. O descenso consiste em obter, a partir desta solução mínima, uma ainda menor, o que nos conduz claramente a uma contradição, provando que A é de fato vazio.

Para ilustrar este método consideremos o seguinte

Exemplo 1 (Fermat). *Demonstrar que a equação $x^4 + y^4 = z^2$ não possui soluções inteiras positivas.*

Solução: Suponhamos que $x^4 + y^4 = z^2$ possui uma solução inteira com $x, y, z > 0$. Logo existe uma solução (a, b, c) na qual c é mínimo. Em particular, temos que a e b são primos entre si, pois se $d = \text{mdc}(a, b) > 1$ poderíamos substituir (a, b, c) por $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d^2})$ e obter uma solução com c menor. De $(a^2)^2 + (b^2)^2 = c^2$ temos portanto que (a^2, b^2, c) é uma tripla pitagórica primitiva e assim existem inteiros positivos m e n primos relativos tais que

$$a^2 = m^2 - n^2, \quad b^2 = 2mn \qquad \text{e} \qquad c = m^2 + n^2.$$

Temos da primeira equação que (a, n, m) é uma tripla pitagórica primitiva e portanto m é ímpar. Assim, de $b^2 = 2mn$ concluímos que b, e portanto n, é par. Observando ainda que $b^2 = (2n)m$ é um quadrado perfeito e $\text{mdc}(2n, m) =$

1, concluímos que tanto $2n$ como m são quadrados perfeitos, donde podemos encontrar inteiros positivos s e t tais que

$$2n = 4s^2 \qquad \text{e} \qquad m = t^2.$$

Por outra parte, dado que $a^2 + n^2 = m^2$, então existirão inteiros positivos i e j, primos entre si, tais que

$$a = i^2 - j^2, \quad n = 2ij \qquad \text{e} \qquad m = i^2 + j^2.$$

Portanto $s^2 = \frac{n}{2} = ij$, logo i e j serão quadrados perfeitos, digamos $i = u^2$ e $j = v^2$.

Logo temos que $m = i^2 + j^2$, $i = u^2$, $j = v^2$ e $m = t^2$, assim

$$t^2 = u^4 + v^4,$$

isto é, (u, v, t) é outra solução da equação original. Porém

$$t \leq t^2 = m \leq m^2 < m^2 + n^2 = c$$

e $t \neq 0$ porque m é diferente de 0. Isto contradiz a minimalidade de c, o que conclui a demonstração. □

Observemos além disso que, uma vez que esta equação não possui soluções inteiras positivas, então a equação $x^4 + y^4 = z^4$ e, mais geralmente $x^{4n} + y^{4n} = z^{4n}$, não possuem soluções inteiras positivas.

Exemplo 2 (IMO1981). *Encontrar todas as soluções inteiras positivas da equação*

$$m^2 - mn - n^2 = \pm 1.$$

Solução: Note que $m^2 = n^2 + mn \pm 1 \geq n^2 \implies m \geq n$, com igualdade se, e só se, $(m, n) = (1, 1)$, que é claramente uma solução. Agora seja (m, n) uma solução com $m > n$. Demonstremos que $(n, m - n)$ também é solução. Para isto observemos que

$$\begin{aligned} n^2 - n(m-n) - (m-n)^2 &= n^2 - nm + n^2 - m^2 + 2mn - n^2 \\ &= n^2 + nm - m^2 \\ &= -(m^2 - nm - n^2) = \mp 1, \end{aligned}$$

Assim, se temos uma solução (m, n), podemos encontrar uma cadeia descendente de soluções, e este processo parará quando atingirmos uma solução (a, b) com $a = b$, ou seja, a solução $(1, 1)$. Invertendo o processo, encontraremos portanto todas as soluções, isto é, se (m, n) é solução então $(m + n, m)$ é solução. Portanto todas as soluções positivas são

$$(1, 1),\ (2, 1),\ (3, 2), \ldots, (F_{n+1}, F_n), \ldots$$

onde F_n representa o n-ésimo termo da sequência de Fibonacci. □

Exemplo 3 (IMO2003). *Determine todos os pares de inteiros positivos* (a, b) *para os quais*

$$\frac{a^2}{2ab^2 - b^3 + 1}$$

é um inteiro positivo.

SOLUÇÃO: Seja (a, b) uma solução inteira positiva. Logo $2ab^2 - b^3 + 1 \geq 1$, e portanto $a \geq \frac{b}{2}$. No caso $a = \frac{b}{2}$, é claro que obtemos uma solução. Para qualquer outra solução, $a > \frac{b}{2}$ e nesse caso $a^2 \geq 2ab^2 - b^3 + 1 = b^2(2a - b) + 1 > b^2 \implies a > b$.

Agora se $\frac{a^2}{2ab^2 - b^3 + 1} = k \in \mathbb{N}$, então a é raiz do polinômio com coeficientes inteiros

$$x^2 - 2kb^2x + k(b^3 - 1) = 0.$$

Mas este polinômio possui outra solução inteira $a_1 = 2kb^2 - a = \frac{k(b^3-1)}{a} \geq 0$, assim (a_1, b) também é solução do problema se $b > 1$. Supondo que a é a maior raiz, de $a \geq a_1$ teremos que $a \geq kb^2$ e assim

$$a_1 = \frac{k(b^3 - 1)}{a} \leq \frac{k(b^3 - 1)}{kb^2} < b.$$

Desta forma, ou $b = 1$ ou $a_1 = \frac{b}{2}$ e neste último caso $k = \frac{b^2}{4}$ e $a = \frac{b^4}{2} - \frac{b}{2}$. Portanto as soluções do problema são $(a, b) = (l, 2l)$, $(2l, 1)$ ou $(8l^4 - l, 2l)$, com $l \in \mathbb{N}$. □

1.1 Equação de Markov

A equação de Markov é a equação diofantina em inteiros positivos

$$x^2 + y^2 + z^2 = 3xyz.$$

É óbvio que $(1, 1, 1)$ e $(1, 1, 2)$ são soluções da equação. Além disso, como a equação é simétrica, podemos considerar, sem perda de generalidade, somente as soluções com as coordenadas $x \leq y \leq z$ ordenadas de forma não decrescente.

Assim suponhamos que (x, y, z) é uma solução com $x \leq y \leq z$ com $z > 1$. O polinômio quadrático

$$T^2 - 3xyT + (x^2 + y^2) = 0$$

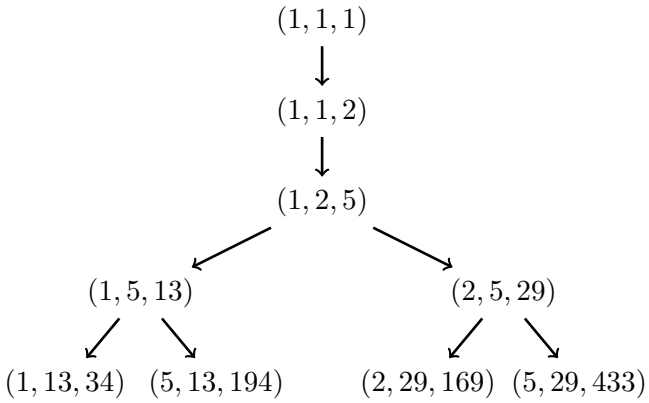
possui duas soluções, e uma dela é z, assim a outra é $z' = 3xy - z = \frac{x^2+y^2}{z} \in \mathbb{Z} \setminus \{0\}$. Vejamos que se $y > 1$ então $z' < y$, e assim (z', x, y) é também solução (menor) da equação de Markov. Para isto, suponhamos por contradição que $\frac{x^2+y^2}{z} = z' \geq y$, isto é, $yz \leq x^2 + y^2 \leq 2y^2$, em particular $z \leq 2y$. Segue que

$$5y^2 \geq y^2 + z^2 = 3xyz - x^2 = x(3yz - x) \geq xy(3z - 1),$$

e portanto $5y \geq x(3z-1)$. Observemos que se $x \geq 2$, então $5y \geq 2(3z-1) \geq 5z$ e portanto $x = y = z = 2$, que não é solução, o que é contraditório. Logo $x = 1$

e $\frac{1+y^2}{y} \geq z$, assim $\frac{1}{y} + y \geq z \geq y$. Portanto ou temos $\frac{1}{y} + y = z$, e neste caso $y = 1$ e $z = 2$, o que contradiz $y > 1$, ou $y = z$ e substituindo na equação original temos que $1 + y^2 + y^2 = 3y^2$, o que implica que $z = y = 1$, o que contradiz o fato de $z > 1$.

Do fato anterior, temos que dada uma solução da equação de Markov (x, y, z) com $z \geq 2$ é sempre possível encontrar uma solução menor (z', x, y) e este processo somente para quando chegamos à solução $(1, 1, 1)$, isto é, estamos gerando uma árvore de soluções da seguinte forma:



Um importante problema em aberto relacionado com a equação de Markov é o *problema da unicidade*, proposto por Frobenius há cerca de 100 anos em [3] (veja também [1]): para quaisquer inteiros positivos x_1, x_2, y_1, y_2, z com $x_1 \leq y_1 \leq z$ e $x_2 \leq y_2 \leq z$ tais que (x_1, y_1, z) e (x_2, y_2, z) são soluções da equação de Markov temos necessariamente $(x_1, y_1) = (x_2, y_2)$?

Se o problema da unicidade admitir uma solução afirmativa, para cada t real, sua pré-imagem $k^{-1}(t)$ pela função k definida na seção 3.4 consistirá de uma única classe de $GL_2(\mathbb{Z})$-equivalência (veja o exercício 3.10).

1.2 Último Teorema de Fermat

Um dos mais famosos problemas na história da Matemática e talvez um dos que mais inspirou o desenvolvimento de novas teorias é o chamado *último teorema de Fermat*.

Pierre de Fermat, que tinha o costume de fazer anotações nas margens de sua cópia do livro de Diofanto, enunciou o teorema que afirma ser impossível encontrar inteiros positivos x, y, z tais que

$$x^n + y^n = z^n \qquad (*)$$

quando n é um inteiro maior do que 2: "encontrei uma demonstração verdadeiramente maravilhosa para isto, mas a margem é demasiado pequena para contê-la".

Para mostrar a inexistência de soluções de $(*)$, basta considerar os expoentes primos. Muitos casos particulares foram mostrados ao longo da história, os quais se dividem em dois tipos: o primeiro, quando $p \nmid xyz$, e o segundo, mais difícil, quando $p \mid xyz$. De fato, Sophie Germain provou o primeiro caso para

todo primo p tal que $2p+1$ também é primo. Legendre provou o teorema para p primo quando $4p+1, 8p+1, 10p+1, 14p+1$ ou $16p+1$ é primo; com isto, provou o último teorema de Fermat para todo $p < 100$. Em 1849, Kummer obteve uma prova para todos os chamados *primos regulares*. Em 1909 Wieferich provou que se a equação de Fermat tem solução para p, então $2^{p-1} \equiv 1 \pmod{p^2}$; tais primos são chamados *primos de Wieferich*. Mirimanoff e Vandiver provaram respectivamente que p deve satisfazer $3^{p-1} \equiv 1 \pmod{p^2}$ e $5^{p-1} \equiv 1 \pmod{p^2}$, e Frobenius provou este mesmo resultado para 11 e 17 no lugar de 3 e 5.

A demonstração do último teorema de Fermat somente foi obtida depois de mais de trezentos anos após sua formulação. Tal demonstração, devida a Andrew Wiles e Richard Taylor ([6] e [5]), insere-se no contexto mais geral da chamada *conjectura de Taniyama-Shimura-Weil* sobre curvas elípticas, que implica a solução do último teorema de Fermat, como conjecturado por G. Frey em 1985 e provado por K. Ribet em 1986. Esta demonstração envolve ideias bastante avançadas e está muito longe do escopo deste livro. Para uma introdução às técnicas utilizadas na prova, veja [2].

Para dar uma ideia da dificuldade deste problema, vejamos uma prova baseada na de Leonhard Euler para o caso $n = 3$. A demonstração original dada por Euler para o caso $n = 3$ é incompleta já que supõe a fatoração única em irredutíveis para extensões de $\mathbb{Z}$. Começamos com um

Lema 4. *Todas as soluções de $s^3 = a^2 + 3b^2$ em inteiros positivos tais que $\mathrm{mdc}(a, b) = 1$ e s é ímpar são dadas por*

$$s = m^2 + 3n^2, \quad a = m^3 - 9mn^2, \quad b = 3m^2n - 3n^3,$$

com $m + n$ ímpar e $\mathrm{mdc}(m, 3n) = 1$.

Demonstração. É fácil verificar que tais números fornecem uma solução da equação e, além disso,

$$\begin{aligned}\mathrm{mdc}(a, b) &= \mathrm{mdc}(m(m^2 - 9n^2), 3n(m^2 - n^2)) \\ &= \mathrm{mdc}(m^2 - 9n^2, m^2 - n^2) = \mathrm{mdc}(8n^2, m^2 - n^2) = 1.\end{aligned}$$

Reciprocamente, suponhamos que (a, b, s) é solução da equação. Seja p um número primo tal que $p \mid s$. Note que, como $\mathrm{mdc}(a, b) = 1$ e s é ímpar, $p \nmid a$, $p \nmid b$ e $p > 3$. Então $a^2 \equiv -3b^2 \pmod{p}$ e como b é invertível módulo p temos

$$\left(\frac{-3}{p}\right) = 1 \iff \left(\frac{p}{3}\right) = 1 \iff p \equiv 1 \pmod{6}$$

pela lei de reciprocidade quadrática. Sabemos que existem inteiros m_1 e n_1 tais que $p = m_1^2 + 3n_1^2$, e teremos que $p^3 = c^2 + 3d^2$ onde $c = m_1^3 - 9m_1n_1^2$ e $d = 3m_1^2n_1 - 3n_1^3$. Note que $\mathrm{mdc}(p, m_1) = \mathrm{mdc}(p, n_1) = 1$ e $p > 3$ e portanto $\mathrm{mdc}(p, c) = \mathrm{mdc}(p, d) = 1$, como na demonstração acima de que $\mathrm{mdc}(a, b) = 1$.

Procederemos por indução sobre o número de divisores primos de s. Se $s = 1$ o resultado é evidente. O caso em que s tem um divisor primo é exatamente o resultado anterior. Agora, suponhamos que o resultado valha para todo s que

tenha k fatores primos (não necessariamente distintos). Se s tem $k+1$ fatores primos, digamos $s = pt$ com p primo ($p > 3$), observemos que

$$t^3p^6 = s^3p^3 = (a^2+3b^2)(c^2+3d^2) = (ac \pm 3bd)^2 + 3(ad \mp bc)^2.$$

Além disso como

$$\begin{aligned}(ad+bc)(ad-bc) &= (ad)^2 - (bc)^2 = d^2(a^2+3b^2) - b^2(c^2+3d^2) \\ &= p^3(t^3d^2 - b^2),\end{aligned}$$

então $p^3 \mid (ad+bc)(ad-bc)$. Se p divide os dois fatores, teremos que $p \mid ad$ e $p \mid bc$. Lembre que $\text{mdc}(p,c) = \text{mdc}(p,d) = 1$, o que implica que $p \mid a$ e $p \mid b$, o que contradiz a hipótese $\text{mdc}(a,b) = 1$. Assim, p^3 divide exatamente um dos fatores, e tomando adequadamente os sinais teremos que

$$u = \frac{ac \pm 3bd}{p^3}, \quad v = \frac{ad \mp bc}{p^3}$$

são inteiros tais que $t^3 = u^2 + 3v^2$. Como t tem k fatores primos segue por hipótese de indução que

$$t = m_2^2 + 3n_2^2, \quad u = m_2^3 - 9m_2n_2^2, \quad v = 3m_2^2n_2 - 3n_2^3.$$

Agora, dado que $a = uc + 3vd$ e $b = \pm(ud - vc)$, substituindo t, u, v, c e d em termos de m_i e n_i ($i = 1, 2$) em s, a e b e fazendo $m = m_1m_2 + 3n_1n_2$, $n = m_1n_2 - m_2n_1$, obteremos o que queríamos demonstrar. □

O método utilizado por Euler para demonstrar o caso $n = 3$ é basicamente o método de descenso infinito.

Proposição 5. *A equação diofantina $x^3 + y^3 = z^3$ não possui soluções inteiras com $xyz \neq 0$.*

Demonstração. Suponhamos que a equação $x^3 + y^3 = z^3$ possui uma solução com $x, y, z > 0$ e escolhemos está solução de tal forma que xyz seja mínimo. Como qualquer fator comum de dois destes números é também fator do terceiro, podemos afirmar que x, y, z são primos relativos dois a dois. Em particular um de tais números será par.

Note que $x = y$ é impossível pois caso contrário $2x^3 = z^3$ e o expoente da maior potência de 2 do lado direito seria múltiplo de 3, enquanto que do lado esquerdo não. Assim, sem perda de generalidade, podemos assumir que $x > y$.

Suponha primeiro que x e y são ímpares e z par, podemos escrever $x = p+q$ e $y = p-q$ com $p > 0$ e $q > 0$ primos relativos (pois x e y são primos relativos) e de diferente paridade, assim

$$\begin{aligned}x^3 + y^3 &= (x+y)(x^2 - xy + y^2) \\ &= 2p((p+q)^2 - (p+q)(p-q) + (p-q)^2) \\ &= 2p(p^2 + 3q^2).\end{aligned}$$

Portanto $2p(p^2+3q^2)$ é um cubo perfeito. De igual forma, no caso em que z é ímpar e x ou y é par, podemos supor sem perda de generalidade que y é ímpar, e substituindo $z = q+p$ e $y = q-p$ obteremos

$$\begin{aligned} x^3 = z^3 - y^3 &= 2p((p+q)^2 + (p+q)(q-p) + (q-p)^2) \\ &= 2p(p^2+3q^2). \end{aligned}$$

Como p^2+3q^2 é ímpar e $2p(p^2+3q^2)$ é um cubo perfeito temos que p será par. Calculando o máximo comum divisor entre p e p^2+3q^3, obtemos

$$\text{mdc}(p, p^2+3q^2) = \text{mdc}(p, 3q^2) = \text{mdc}(p, 3).$$

Portanto há dois casos: $\text{mdc}(p,3) = 1$ e $\text{mdc}(p,3) = 3$.

No primeiro, existem naturais a e b tais que $a^3 = 2p$ e $b^3 = p^2+3q^2$. Neste caso sabemos, pelo lema 4, que existem inteiros m e n de diferente paridade e primos relativos tais que

$$b = m^2+3n^2, \quad p = m^3 - 9mn^2, \quad q = 3m^2n - 3n^3.$$

Logo $a^3 = 2m(m-3n)(m+3n)$. Observemos que os números $2m$, $m-3n$ e $m+3n$ são primos relativos, logo existem inteiros e, f e g tais que $2m = e^3$, $m-3n = f^3$ e $m+3n = g^3$. Em particular, teremos que $f^3+g^3 = e^3$. Como

$$efg = a^3 = 2p \leq x+y < xyz,$$

teremos uma solução menor, o que contradiz a escolha de x, y, z.

No caso em que $3 \mid p$, então $p = 3r$ com $\text{mdc}(r,q) = 1$, logo $z^3 = 18r(3r^2+q^2)$ ou $x^3 = 18r(3r^2+q^2)$ e portanto existem inteiros positivos a e b tais que $18r = a^3$ e $3r^2+q^2 = b^3$. De novo, existiriam inteiros m e n tais que

$$b = m^2+3n^2, \quad q = m^3 - 9mn^2, \quad r = 3m^2n - 3n^3.$$

Daqui segue que $a^3 = 27(2n)(m-n)(m+n)$. De igual forma teremos que os números $2n$, $m-n$ e $m+n$ são primos relativos, portanto existem inteiros positivos e, f e g tais que

$$2n = e^3, \quad m-n = f^3, \quad m+n = g^3.$$

Segue que $e^3+f^3 = g^3$, que também contradiz a minimalidade da solução (x,y,z). □

Exemplo 6. *Demonstrar que a equação* $x^2+432 = y^3$ *não tem soluções racionais diferentes de* $(\pm 36, 12)$.

SOLUÇÃO: Suponhamos que a equação possui uma solução (a,b) com $b \neq 12$. Como a e b são racionais, então $\frac{a}{36} = \frac{k}{n} \neq \pm 1$ e $\frac{b}{12} = \frac{m}{n} \neq 1$ com $k, m, n \in \mathbb{Z}$. Seja $u = n+k \neq 0$, $v = n-k \neq 0$ e $w = 2m$. Como

$$u^3+v^3-w^3 = 2n^3+6nk^2-8m^3$$

e $k = \frac{an}{36}, m = \frac{bn}{12}$, substituindo temos

$$u^3+v^3-w^3 = 2n^3 + \frac{n^3a^2}{6^3} - \frac{n^3b^3}{6^3} = \frac{n^3}{216}(432+a^2-b^3) = 0.$$

o que gera uma solução não trivial da equação $x^3+y^3 = z^3$, um absurdo. □

Problemas Propostos

Problema 7. *Demonstrar que não existe um triângulo retângulo com lados inteiros tal que sua área seja um quadrado perfeito.*

Problema 8. *Encontrar todos os pares* (n, m) *de números inteiros tais que* $n \mid m^2 + 1$ *e* $m \mid n^2 + 1$.

Problema 9 (IMO1987)**.** *Seja* n *um inteiro maior ou igual a* 2*. Mostre que se* $k^2 + k + n$ *é primo para todo* k *tal que* $0 \leq k \leq \sqrt{\frac{n}{3}}$*, então* $k^2 + k + n$ *é primo para todo* k *tal que* $0 \leq k \leq n - 2$.

Problema 10 (IMO1988)**.** *Dados inteiros* a *e* b *tais que o número* $ab + 1$ *divide* $a^2 + b^2$*, demonstrar que*

$$\frac{a^2 + b^2}{ab + 1}$$

é um quadrado perfeito.

Problema 11 (IMO2007)**.** *Prove que se* a *e* b *são inteiros positivos tais que* $4ab - 1 \mid (4a^2 - 1)^2$ *então* $a = b$.

Problema 12. *Demonstrar que a equação* $3x^2 + 1 = y^3$ *não tem soluções racionais diferentes de* $x = \pm 1$ *e* $y = 1$.

Problema 13. *Demonstrar que a equação* $x^3 + y^3 + z^3 = 1$ *possui infinitas soluções inteiras.*

Problema 14. *Demonstrar que a equação* $x^3 + y^3 + z^3 = n$ *com* $n = 9k \pm 4$ *não possui soluções inteiras.*

Problema 15. *Demonstrar que a equação* $x^3 + y^3 + z^3 = t^3$ *possui infinitas soluções inteiras positivas primitivas (i.e., com* $\mathrm{mdc}(x, y, z, t) = 1$*).*

Problema 16. *Demonstrar que a equação* $x^3 + y^3 = 2z^3$ *não possui soluções inteiras positivas não triviais (i.e. além das com* $x = y = z$*).*

Dicas e Soluções

Em breve.

Referências

[1] J. W. S. Cassels, *An introduction to Diophantine approximation*, Cambridge Tracts in Mathematics and Mathematical Physics 45, Hafner Publishing Co. (1972)

[2] G. Cornell, J. H. Silverman e G. Stevens, *Modular Forms and Fermat's Last Theorem*, Springer-Verlag (2009).

[3] G. Frobenius, *Über die Markoffschen Zahlen*, Preuss. Akad. Wiss. Sitzungberichte (1913), 458–487; disponível também em G. Frobenius, *Gesammelte Abhandlungen*, vol. 3, Springer (1968), 598–627.

[4] F. E. Brochero Martinez, C. G. Moreira, N. C. Saldanha, E. Tengan - Teoria dos Números - um passeio com primos e outros números familiares pelo mundo inteiro, Projeto Euclides, IMPA, 2010.

[5] R. Taylor e A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) 141 (1995), no. 3, 553–572.

[6] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) 141 (1995), no. 3, 443–551.